

Oracle Health Sciences Empirica Signal Security Guide



Release 9.2.1
F58612-01



Copyright © 2002, 2022, Oracle and/or its affiliates.

This software and related documentation are provided under a license agreement containing restrictions on use and disclosure and are protected by intellectual property laws. Except as expressly permitted in your license agreement or allowed by law, you may not use, copy, reproduce, translate, broadcast, modify, license, transmit, distribute, exhibit, perform, publish, or display any part, in any form, or by any means. Reverse engineering, disassembly, or decompilation of this software, unless required by law for interoperability, is prohibited.

The information contained herein is subject to change without notice and is not warranted to be error-free. If you find any errors, please report them to us in writing.

If this is software or related documentation that is delivered to the U.S. Government or anyone licensing it on behalf of the U.S. Government, then the following notice is applicable:

U.S. GOVERNMENT END USERS: Oracle programs (including any operating system, integrated software, any programs embedded, installed or activated on delivered hardware, and modifications of such programs) and Oracle computer documentation or other Oracle data delivered to or accessed by U.S. Government end users are "commercial computer software" or "commercial computer software documentation" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, the use, reproduction, duplication, release, display, disclosure, modification, preparation of derivative works, and/or adaptation of i) Oracle programs (including any operating system, integrated software, any programs embedded, installed or activated on delivered hardware, and modifications of such programs), ii) Oracle computer documentation and/or iii) other Oracle data, is subject to the rights and limitations specified in the license contained in the applicable contract. The terms governing the U.S. Government's use of Oracle cloud services are defined by the applicable contract for such services. No other rights are granted to the U.S. Government.

This software or hardware is developed for general use in a variety of information management applications. It is not developed or intended for use in any inherently dangerous applications, including applications that may create a risk of personal injury. If you use this software or hardware in dangerous applications, then you shall be responsible to take all appropriate fail-safe, backup, redundancy, and other measures to ensure its safe use. Oracle Corporation and its affiliates disclaim any liability for any damages caused by use of this software or hardware in dangerous applications.

Oracle, Java, and MySQL are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Inside are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. AMD, Epyc, and the AMD logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group.

This software or hardware and documentation may provide access to or information about content, products, and services from third parties. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third-party content, products, and services unless otherwise set forth in an applicable agreement between you and Oracle. Oracle Corporation and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services, except as set forth in an applicable agreement between you and Oracle.

Contents

Preface

Documentation accessibility	v
Related resources	v
Access to Oracle Support	v
Additional copyright information	v

1 Overview

General security principles	1-1
-----------------------------	-----

2 Installing and configuring the Oracle Empirica Signal software

Configure Oracle WebLogic Server to use TLS	2-2
Use a separate port for the Oracle Empirica Signal application	2-2
Enable only what is required	2-2
Execute scripts without passwords on the command line	2-2
Reset the Read Only attribute	2-3
Use secure Oracle Empirica Signal database and Oracle Empirica Topics credentials	2-3
Turn on the HttpOnly flag for session cookies within Oracle WebLogic Server for the Oracle Empirica Signal software	2-3
Establish best practices for downloading data	2-3
Route email to a secure address	2-3
Use TLS	2-4
Encrypt the database connection	2-4
Install the Oracle Empirica Signal application on a separate managed server	2-4
Install the Oracle Analytics Server	2-4
Installing the Oracle Database software	2-5
Patch the database regularly and apply security updates	2-5
Patch the Oracle Java SE regularly and apply security updates	2-5
Allow database passwords to expire, and change default passwords	2-6
Configure components to use FIPS 140-2 compliant cryptographic implementations	2-6
Enable TDE in the database	2-6

3 Overview of security features

Oracle Empirica Topics security	3-1
Authentication methods	3-2
Password requirements	3-2
Disabling user accounts	3-3
Auditing	3-3
Oracle Database client identifier	3-3
User access control	3-3
Assigning roles	3-4
Granting permissions	3-4
Publishing objects	3-4
Oracle Empirica Topics	3-4
User session timeout	3-5

Preface

This preface contains the following sections:

- [Documentation accessibility](#)
- [Related resources](#)
- [Access to Oracle Support](#)
- [Additional copyright information](#)

Documentation accessibility

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website at <http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc>.

Related resources

All documentation and other supporting materials are available on the [Oracle Help Center](#).

Access to Oracle Support

Oracle customers that have purchased support have access to electronic support through Support Cloud.

Contact our Oracle Customer Support Services team by logging requests in one of the following locations:

- English interface of Oracle Health Sciences Customer Support Portal (<https://hsgbu.custhelp.com/>)
- Japanese interface of Oracle Health Sciences Customer Support Portal (<https://hsgbu-jp.custhelp.com/>)

You can also call our 24x7 help desk. For information, visit <http://www.oracle.com/us/support/contact/health-sciences-cloud-support/index.html> or visit <http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs> if you are hearing impaired.

Additional copyright information

This documentation may include references to materials, offerings, or products that were previously offered by Phase Forward Inc. Certain materials, offerings, services, or products may no longer be offered or provided. Oracle and its affiliates cannot be held responsible for any such references should they appear in the text provided.

1

Overview

Oracle Empirica Signal is a web application that provides a data mining environment for detecting signals, uncovering patterns, and recognizing trends in adverse event report data. Using the Oracle Empirica Signal application, industry and pharmacovigilance professionals can manage the review, processing, and response to drug and vaccine safety signals.

To protect the integrity and confidentiality of your data, install the Oracle Empirica Signal software and system components using secure installation methods. After installation, manage and monitor your system to ensure that your data is protected from unauthorized access and misuse.

The following chapters provide secure installation and configuration guidelines and describe the security features provided in Oracle Empirica Signal to help you manage and monitor your system.

- [General security principles](#)
These are basic security principles to implement.

General security principles

These are basic security principles to implement.

- **Require strong, complex application and database passwords.**
Create a password policy to establish password requirements. For example, require a minimum password length and at least one of each of the following types of characters:
 - Alphabetic
 - Numeric
 - Non-alphanumeric
 - Upper-case character
 - Lower-case character
- **Keep passwords secure.**
When you initially create user accounts in the Oracle Empirica Signal software, send users their user name and initial password in separate email messages. Instruct your users not to share or write down passwords, or to store passwords in files on their computers. Additionally, require users to change their passwords upon first use.
- **Keep software up-to-date.**
Keep all software versions current by installing the latest patches for all components, including all critical security updates.
- **Implement the principle of least privilege.**
In implementing the principle of least privilege, you grant users the fewest number of permissions needed to perform their jobs. You should also review user permissions regularly to determine their relevance to users' current job responsibilities.
- **Monitor system activity.**
Review user audit records regularly to determine which user activities constitute normal use, and which may indicate unauthorized use or misuse.

- **Promote policy awareness.**
Ensure that your employees are aware of Acceptable Use policies, best practices, and standard operating procedures that are relevant to the Oracle Empirica Signal software.

2

Installing and configuring the Oracle Empirica Signal software

The Oracle Empirica Signal *Installation and Upgrade Instructions* include procedures that install the application and system components into a secure state by default.

The accounts that you create during the installation also have restrictive permissions by default. In addition to performing the standard installation procedures, you can perform the steps in this chapter to secure the Oracle Empirica Signal software.

- [Configure Oracle WebLogic Server to use TLS](#)
Before you install the Oracle Empirica Signal software, obtain a TLS certificate, install the certificate on the application server, and configure Oracle WebLogic Server to use the certificate.
- [Use a separate port for the Oracle Empirica Signal application](#)
Install the Oracle Empirica Signal application so that the application listens on a different port than the Oracle WebLogic Server administration console and Oracle Enterprise Manager console. The *Installation and Upgrade Instructions* describe how to configure the Oracle Empirica Signal application to use a unique port.
- [Enable only what is required](#)
When you have completed the installation, disable features that you might not use, such as LDAP, in the site options.
- [Execute scripts without passwords on the command line](#)
When you are required to authenticate to your Oracle Database during the Oracle Empirica Signal installation, do not provide database account passwords as arguments from the Command Prompt.
- [Reset the Read Only attribute](#)
The standard Oracle Empirica Signal installation requires you to make several files editable.
- [Use secure Oracle Empirica Signal database and Oracle Empirica Topics credentials](#)
The Oracle Empirica Signal *Installation and Upgrade Instructions* include directions for configuring database and Oracle Empirica Topics credentials.
- [Turn on the HttpOnly flag for session cookies within Oracle WebLogic Server for the Oracle Empirica Signal software](#)
Using the HttpOnly flag when generating a cookie helps mitigate the risk of a client-side script accessing the protected cookie.
- [Establish best practices for downloading data](#)
The Oracle Empirica Signal software provides the option to download table data to a Microsoft Excel spreadsheet or to other file types, such as PDF.
- [Route email to a secure address](#)
In the Oracle Empirica Signal software, provide secure email addresses for the From Email Address, and Error Email site options.

- [Use TLS](#)
Oracle strongly recommends configuring Oracle WebLogic Server to use TLS and accessing the Oracle Empirica Signal software using only TLS connections. For more information, see the *Installation and Upgrade Instructions*.
- [Encrypt the database connection](#)
If you install the Oracle Empirica Signal software and Oracle Database software on different servers, secure configuration requires encryption of the communication channel between the servers.
- [Install the Oracle Empirica Signal application on a separate managed server](#)
Do not install the Oracle Empirica Signal application on the Oracle WebLogic Server administration server.
- [Install the Oracle Analytics Server](#)
You must install and configure Oracle Analytics and its components securely.
- [Installing the Oracle Database software](#)
This sections describes how to install the Oracle Database software securely.
- [Secure Oracle Empirica Topics Development](#)
Follow secure development guidelines for Oracle Empirica Topics development.

Configure Oracle WebLogic Server to use TLS

Before you install the Oracle Empirica Signal software, obtain a TLS certificate, install the certificate on the application server, and configure Oracle WebLogic Server to use the certificate.

Use a separate port for the Oracle Empirica Signal application

Install the Oracle Empirica Signal application so that the application listens on a different port than the Oracle WebLogic Server administration console and Oracle Enterprise Manager console. The *Installation and Upgrade Instructions* describe how to configure the Oracle Empirica Signal application to use a unique port.

Enable only what is required

When you have completed the installation, disable features that you might not use, such as LDAP, in the site options.

Execute scripts without passwords on the command line

When you are required to authenticate to your Oracle Database during the Oracle Empirica Signal installation, do not provide database account passwords as arguments from the Command Prompt.

The standard installation instructions provide appropriate script execution examples.

Reset the Read Only attribute

The standard Oracle Empirica Signal installation requires you to make several files editable.

After the installation completes, make sure that you reset the file permissions to **Read Only** unless explicitly instructed otherwise in the *Installation and Upgrade Instructions*.

Use secure Oracle Empirica Signal database and Oracle Empirica Topics credentials

The Oracle Empirica Signal *Installation and Upgrade Instructions* include directions for configuring database and Oracle Empirica Topics credentials.

To ensure secure installation, use passwords that observe complexity standards.

Turn on the HttpOnly flag for session cookies within Oracle WebLogic Server for the Oracle Empirica Signal software

Using the HttpOnly flag when generating a cookie helps mitigate the risk of a client-side script accessing the protected cookie.

Perform these steps on the application server.

To turn on the HttpOnly flag for session cookies:

1. Navigate to the <INSTALL_DIR>/Signal/WEB-INF directory.
2. Open the `weblogic.xml` file, and locate the <session-descriptor> section.
3. If the section does not contain the following element, add the element:

```
<wls:cookie-http-only>true</wls:cookie-http-only>
```

Establish best practices for downloading data

The Oracle Empirica Signal software provides the option to download table data to a Microsoft Excel spreadsheet or to other file types, such as PDF.

Establish best practices for downloading data to ensure the data remains secure outside the Oracle Empirica Signal software.

Route email to a secure address

In the Oracle Empirica Signal software, provide secure email addresses for the From Email Address, and Error Email site options.

Consider providing email addresses that are not routed over the Internet.

Use TLS

Oracle strongly recommends configuring Oracle WebLogic Server to use TLS and accessing the Oracle Empirica Signal software using only TLS connections. For more information, see the *Installation and Upgrade Instructions*.

To ensure that your use of TLS is secure, perform the following steps:

- Disable the use of vulnerable TLS protocols by adding the following JVM option to the `JAVA_OPTIONS` settings in the `setDomainEnv.sh` file, for example:
`-Dweblogic.security.SSL.minimumProtocolVersion=TLSv1.2`

You can find the `setDomainEnv.sh` file in a location such as: `/u01/app/oracle/Middleware/user_projects/domains/empirica/bin/setDomainEnv.sh`

- Enable only strong ciphers in the Oracle WebLogic Server `config.xml` file by listing only strong ciphers in the SSL section of the file. For more information, see the Open Web Application Security Project website:

http://www.owasp.org/index.php/Transport_Layer_Protection_Cheat_Sheet#Rule_-_Only_Support_Strong_Cryptographic_Ciphers

Encrypt the database connection

If you install the Oracle Empirica Signal software and Oracle Database software on different servers, secure configuration requires encryption of the communication channel between the servers.

For more information, see the section about configuring the thin JDBC client network in the *Oracle Database Security Guide*:

<https://docs.oracle.com/en/database/oracle/oracle-database/19/dbseg/configuring-thin-jdbc-client-network.html>

Install the Oracle Empirica Signal application on a separate managed server

Do not install the Oracle Empirica Signal application on the Oracle WebLogic Server administration server.

Install the application on a separate managed server in the WebLogic domain. When you use a separate managed server for the application, you access the application on a different port than the port for the administration server.

Install the Oracle Analytics Server

You must install and configure Oracle Analytics and its components securely.

For information on installing and configuring Oracle Analytics and its components securely, see the *Security Guide for Oracle Analytics Server* at:

<https://docs.oracle.com/en/middleware/bi/analytics-server/install-config-oas/index.html>

Installing the Oracle Database software

This section describes how to install the Oracle Database software securely.

For more information and additional guidelines for securely installing and managing the Oracle database, see the Oracle *Database Security Guide*:

- <https://docs.oracle.com/en/database/oracle/oracle-database/19/dbseg/index.html>

Follow these steps to install the Oracle Database software securely:

- [Patch the database regularly and apply security updates](#)
Periodically check the security site on Oracle Technology Network for details about security alerts for Oracle products.
- [Patch the Oracle Java SE regularly and apply security updates](#)
Periodically check the security site on Oracle Technology Network for security alerts about Oracle Java SE.
- [Allow database passwords to expire, and change default passwords](#)
Oracle Database is installed with several default database user accounts, such as **SYS** and **SYSTEM**.
- [Configure components to use FIPS 140-2 compliant cryptographic implementations](#)
You can configure the Oracle Database and Oracle WebLogic Server used with the Oracle Empirica Signal application to use FIPS 140-2 approved and validated encryption modules.
- [Enable TDE in the database](#)
You must protect sensitive data by encryption. Oracle Empirica Signal 9.2.1 supports encrypted tablespaces in an Oracle Database where Transparent Data Encryption (TDE) is enabled.

Patch the database regularly and apply security updates

Periodically check the security site on Oracle Technology Network for details about security alerts for Oracle products.

For more information, see the following link:

<http://www.oracle.com/technetwork/topics/security/alerts-086861.html>

Patch the Oracle Java SE regularly and apply security updates

Periodically check the security site on Oracle Technology Network for security alerts about Oracle Java SE.

For more information, see the following link:

<http://www.oracle.com/technetwork/topics/security/alerts-086861.html>

Allow database passwords to expire, and change default passwords

Oracle Database is installed with several default database user accounts, such as **SYS** and **SYSTEM**.

After the database is installed successfully, the Database Configuration Assistant automatically locks most built-in database user accounts and marks them as expired. After the accounts expire, you should configure strong and secure passwords for them.

Configure components to use FIPS 140-2 compliant cryptographic implementations

You can configure the Oracle Database and Oracle WebLogic Server used with the Oracle Empirica Signal application to use FIPS 140-2 approved and validated encryption modules.

For more information, see the following link:

<http://www.oracle.com/technetwork/topics/security/oracle-fips140-validations-100923.html>

Enable TDE in the database

You must protect sensitive data by encryption. Oracle Empirica Signal 9.2.1 supports encrypted tablespaces in an Oracle Database where Transparent Data Encryption (TDE) is enabled.

Before upgrading from Oracle Empirica Signal 8.1.x to Oracle Empirica Signal 9.2.1, perform the following steps:

1. Export all tablespaces from the 8.1.x database.
2. Import all tablespaces from the 8.1.x database into encrypted tablespaces in the 9.1 database.
3. Enable TDE in the 9.1 database.

For more information about TDE, see:

<http://www.oracle.com/us/products/database/options/advanced-security/overview/index.html>

Secure Oracle Empirica Topics Development

Follow secure development guidelines for Oracle Empirica Topics development.

See the *Secure Development Guidelines* chapter in the Oracle Empirica Topics API Guide.

3

Overview of security features

The Oracle Empirica Signal software provides the following security features to help you secure your system:

- [Oracle Empirica Topics security](#)
You must support Web Services Security. Define a Web Services Security User Name Token Policy and include the user name and password with each SOAP message.
- [Authentication methods](#)
The Oracle Empirica Signal software requires users to authenticate by logging in with a unique user name and password.
- [Auditing](#)
The User Activity Audit Trail tracks user activity that occurs in the application, capturing detailed information for user actions and providing you with an easily accessible, historical account of user activity.
- [Oracle Database client identifier](#)
For each connection to the Oracle Database, Oracle Empirica Signal sets the `CLIENT_IDENTIFIER` attribute to the **ID** value for the currently connected user.
- [User access control](#)
The Oracle Empirica Signal software allows you to implement user access control. Using roles and permissions, you can restrict user access to only the activities that are necessary for users to perform their job responsibilities.
- [User session timeout](#)
The Oracle Empirica Signal application cancels user sessions that have been inactive for a specified period of time.

Oracle Empirica Topics security

You must support Web Services Security. Define a Web Services Security User Name Token Policy and include the user name and password with each SOAP message.

Store the Oracle Empirica Topics web service user name and password in the Oracle WebLogic Server credential store. The Oracle Empirica Topics web service uses Oracle WebLogic Server to validate the Web Services Security User Name Token Policy for each request.

If the web service credentials are incorrect or the Web Services Security User Name Token Policy has not been set, the Oracle Empirica Topics server returns an exception. The Oracle Empirica Topics web service becomes unavailable for that application.

For information on how to set up the user name token policy and add credentials to the credential store, see *Set up the Oracle Empirica Topics web service security policy in the Oracle Empirica Signal Installation and Upgrade Instructions*.

Authentication methods

The Oracle Empirica Signal software requires users to authenticate by logging in with a unique user name and password.

You can use the following authentication methods:

- **Local**—User information stored in Oracle Empirica Signal is used for authentication.
- **Single Sign-On (SSO)**—User information stored in a single sign-on application is used for authentication. For example, you might use Oracle Health Sciences Identity and Access Management Service or Oracle Access Manager for single sign-on.
- **LDAP**—User information stored in a Lightweight Directory Access Protocol (LDAP) directory is used for authentication.

With local and LDAP authentication, Oracle Empirica Signal captures successful and failed login attempts in the User Activity Audit Trail. For more information, see [Auditing](#).

In addition, when a locally authenticated user exceeds the allowable number of login attempts that you set in your password requirements, Oracle Empirica Signal sends an account lockout email notification to the site administrator.

For more information on configuring and implementing authentication methods, see Ways to administer users in the Oracle Empirica Signal *User Guide and Online Help*.

Authentication is involved in:

- [Password requirements](#)
The Oracle Empirica Signal software provides password options that you can select to establish a password policy for the user accounts for your local users.
- [Disabling user accounts](#)
When an employee leaves your organization, the Oracle Empirica Signal software allows you to disable the employee's user account to prevent unauthorized system access.

Password requirements

The Oracle Empirica Signal software provides password options that you can select to establish a password policy for the user accounts for your local users.

Using the options in the table below, you can require specific password content, complexity, and expiration. The Oracle Empirica Signal software provides the following password options and default values. You can edit the default values to suit the requirements of your organization.

Option	Default value	Option	Default value
Expiration	90 days	Expiration warning	15 days
Minimum Length	8 characters	Minimum Numeric	1
Number of Attempts Allowed	3	Minimum Non-alphanumeric	1

Option	Default value	Option	Default value
Number of Passwords Retained	8	Minimum Lowercase	1
Minimum Alphabetic	1	Minimum Uppercase	1

If you use single sign-on (SSO) for authentication, you should set similar password requirements in your SSO application.

Disabling user accounts

When an employee leaves your organization, the Oracle Empirica Signal software allows you to disable the employee's user account to prevent unauthorized system access.

Auditing

The User Activity Audit Trail tracks user activity that occurs in the application, capturing detailed information for user actions and providing you with an easily accessible, historical account of user activity.

Using the User Activity Audit Trail, you can better enforce your company's security policy and monitor your system for attempts at unauthorized actions or misuse.

Audited user activity is retained indefinitely. You cannot modify or delete audit records through the Oracle Empirica Signal software. The software auditing feature is a standard feature that cannot be disabled.

Oracle Empirica Signal also supports Oracle Database Fine Grain Auditing. Using the DBMS_FGA package, you can set a policy to audit all activities on tables. For details refer to Oracle Database documentation.

Oracle Database client identifier

For each connection to the Oracle Database, Oracle Empirica Signal sets the `CLIENT_IDENTIFIER` attribute to the **ID** value for the currently connected user.

Oracle activities that include `CLIENT_IDENTIFIER`, such as the SQL trace files, performance tuning tools, and enabled audit policies, reflect the Oracle Empirica Signal user **ID**.

User access control

The Oracle Empirica Signal software allows you to implement user access control. Using roles and permissions, you can restrict user access to only the activities that are necessary for users to perform their job responsibilities.

Before implementing user access control, establish an access control policy based on business and security requirements for each user. Review your access control policy periodically to determine if changes to roles and permissions are necessary.

User access control is involved in:

- [Assigning roles](#)
During installation, several built-in roles are created.
- [Granting permissions](#)
The Oracle Empirica Signal software defines permissions that grant or restrict user access to different application features.
- [Publishing objects](#)
You can control user access to objects, such as analysis runs and report outputs, by publishing the objects to specific login groups. By default, the publication level of every newly created object is Private.
- [Oracle Empirica Topics](#)
You can add a layer of security on Oracle Empirica Topics by creating work teams.

Assigning roles

During installation, several built-in roles are created.

The roles are designed for least privilege and separation of duties. You can modify the permissions assigned to the roles and create new roles, if needed.

Granting permissions

The Oracle Empirica Signal software defines permissions that grant or restrict user access to different application features.

When you assign a role to a user, the user receives all the permissions assigned to the role. Review the permissions assigned to roles to make sure users can perform only the tasks relevant to their job responsibilities.

You can also assign permissions to users.

Publishing objects

You can control user access to objects, such as analysis runs and report outputs, by publishing the objects to specific login groups. By default, the publication level of every newly created object is Private.

Users without the Administer Users permission can publish only objects they have created. Users with the Administer Users permission can publish objects that they or any users in their login group created.

Superusers can publish any object.

For more information on user access control, see the Oracle Empirica Signal User Guide and Online Help.

Oracle Empirica Topics

You can add a layer of security on Oracle Empirica Topics by creating work teams.

Work teams enable different groups of users to view a topic. Within a work team, you can give users different work team permissions, which determine the level of access users have to topics that are visible to them.

Additionally, you can configure Oracle Empirica Topics email notifications to alert individual users or work teams of significant changes to topics. Oracle Empirica Topics email notifications optionally include topic or action fields from the topic workflow configuration. Before including fields in email notifications, you should ensure that the resulting email messages do not contain sensitive or confidential information.

A user can view changes to topics in the history of a topic or action or both, and can track the deleted attachments and actions in the audit trail.

User session timeout

The Oracle Empirica Signal application cancels user sessions that have been inactive for a specified period of time.

To change the default user session timeout value, see [Set up the webvdme.properties file for Oracle Empirica Signal in the *Installation and Upgrade Instructions*](#).